**Alunos: Vinicius Coelho, Caio Domingues**

**Matricula: 201700121, 201700550**

**1ª Questão**

Pode acarretar em perda de tempo, queda de produtividade, perda significativa de dinheiro, horas de trabalho, devastação da credibilidade ou oportunidades, empresa não habilitada em competir.

**2ª Questão**

Ela busca reduzir os riscos de vazamento de informações, fraudes em arquivos, bancos de dados, erros humanos e operacionais, roubo de informações, ou qualquer outra ameaça que possa prejudicá-la.

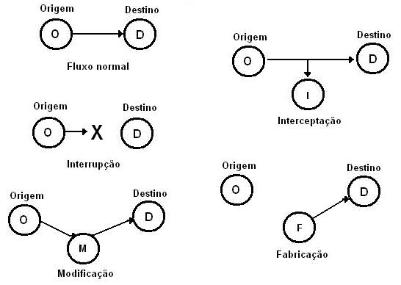
**3ª Questão**

* **Confidencialidade** - Significa proteger informações contra sua revelação para alguém não autorizado.
* **Integridade** - Evitar que dados sejam apagados ou alterados sem a permissão do responsável pela administração do servidor.
* **Disponibilidade** - Garantir o funcionamento do serviço de informação aos usuários autorizados, e a duplicação de sistemas e serviços(RAID).
* **Consistência** - Certificar-se de que o sistema atua de acordo com a expectativa do usuário.
* **Isolamento** - Controla o acesso ao sistema e garante que somente os usuários autorizados possuam acesso ao sistema.
* **Auditoria** - Protege os sistemas contra erros e atos cometidos por usuários não autorizados.
* **Confiabilidade** - Garante que, mesmo em condições adversas, o sistema atuará conforme esperado.
* **Legalidade** - A informação deve estar em conformidade com os preceitos da legislação em vigor.

**4ª Questão**

As políticas de segurança, em relação a arquitetura de servidores Web, devem fornecer meios para garantir que as informações de uso restrito não serão acessadas, copiadas ou codificadas por pessoas não autorizadas. Dessa forma uma das maneiras de evitar o acesso indevido é através da codificação da informação.

**5ª Questão**



**6ª Questão**

Objetiva garantir a segurança e a priorização de recursos, focando os

investimentos nas informações mais importantes para a organização.

**7ª Questão**

**Confidencialidade:** Classificar a informação levando em consideração a gravidade do impacto ou prejuízo que a revelação não autorizada da mesma trará para a organização.

 **Confidencial** – toda informação considerada de alto risco para a

empresa, pois sua revelação não autorizada pode trazer graves

prejuízos.

 **Restrita** – toda informação considerada de médio e baixo risco para

a empresa, pois sua revelação não autorizada pode trazer

prejuízos a uma determinada área da empresa.

 **Pública** – toda informação considerada de nenhum risco para a

empresa e sua revelação não autorizada não traz nenhum prejuízo.

**Integridade:** Classificar a informação levando em consideração a gravidade do

impacto ou dos prejuízos que a modificação não autorizada da informação

trará.

 **Crítica** – toda informação de alto risco para a empresa. Não pode

ser alterada sem prévia autorização.

 **Não-Crítica** – toda informação que, se alterada sem prévia

autorização, não representa nenhum risco para a empresa.

**Disponibilidade:** Classificar as informações levando em consideração a gravidade do impacto ou dos prejuízos que a indisponibilidade da informação trará.

 **Vital** – toda informação de alto risco para a empresa. Esta

informação precisa estar sempre disponível.

** Não-Vital** – toda informação que, em caso de indisponibilidade, não

representa nenhum risco para a empresa.

**Classificação Padrão:** Todas as informações que não forem classificadas deverão entrar no nível padrão de classificação.

**8ª Questão**

* **Proprietários da Informação** – gestores das áreas geradoras das

informações, sendo os proprietários, responsáveis por classificar,

desclassificar, redefinir os níveis de classificação das informações, dentro

da arquitetura dos servidores Web específicos.

* **Custodiantes** – são os responsáveis por guardar e recuperar as

informações classificadas e por prover e administrar os acessos às

informações devidamente solicitadas pelos proprietários.

**9ª Questão**

* **Ameaças à Integridade** – ameaças ambientais (fogo, água, terremoto e etc), erros humanos, fraudes, falhas no processamento.
* **Ameaças de Indisponibilidade** – falhas em sistemas ou nos diversos ambientes computacionais.
* **Ameaças de divulgação da informação** – divulgação de informações premeditada ou acidental.
* **Ameaças por alterações não autorizadas** – alteração premeditada ou acidental do conteúdo das informações do sistema.

**10ª Questão**

**Prevenção:**

• **Proteção de Hardware** – chamado de segurança física, impede acessos físicos não autorizados à infraestrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos possíveis quando se está fisicamente no local.

• **Proteção de arquivos e dados** – providenciado por autenticação (onde é verificada a identidade do usuário), controle de acesso (só são

disponibilizadas as transações pertinentes ao usuário) e antivírus (garante a proteção do sistema contra programas maliciosos).

• **Proteção de perímetro** – ferramentas de firewall cuidam deste aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

**Professor**

**Detecção:**

• **Alertas** – sistemas de detecção de intrusos (IDS) alertam os

administradores e responsáveis pela segurança da rede sobre qualquer

sinal de invasão ou mudança suspeita no comportamento da rede que

possa significar um padrão de ataque. Os avisos podem ser via mail,

mensagem no terminal do administrador do servidor, etc.

• **Auditoria** – periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Pode ser realizado por

ferramentas que procuram, por exemplo, modificações no tamanho dos

arquivos de senhas, usuários nativos, etc.

**Rafael Teixeira**  rafael.teixeira@foa.org.br

**Recuperação:**

• **Cópia de Segurança de Dados (Backup)** – manter sempre atualizados e testados os arquivos de segurança de dados em mídia confiável e separado dos servidores.

**• Aplicações de Backup** – ferramentas que proporcionam a recuperação rápida e confiável dos dados mais atualizados em caso de perda dos dados originais do sistema.

• **Backup de Hardware** – servidor reserva, no-break reserva, linha de

dados/comunicação reserva. Podem ser justificados levando-se em conta o custo de uma parada de sistema e determinando-se a importância da informática para a organização.